Lupa

Nathalia Afonso <nathalia@lupa.news>

Levantamento que fala sobre golpes - Agência Lupa

Adriana Mompean <adriana.mompean@febraban.org.br> 13 de julho de 2021 14:23
Para: Nathalia Afonso <nathalia@lupa.news>
Cc: Imprensa FEBRABAN <imprensa.febraban@febraban.org.br>

Oi Nathalia, tudo bem?

Segue o material solicitado. É o mais atualizado que temos.

Abs,

FEBRABAN

Golpe da falsa central telefônica e falso funcionário cresce 340% no primeiro bimestre do ano

Ataques de phishing tiveram aumento de 100% nos dois primeiros meses de 2021 e também

estão entre os golpes mais aplicados no começo do ano, juntamente com o do falso motoboy

Os criminosos têm aproveitado a maior permanência das pessoas em casa e o amento das transações digitais por causa da pandemia do novo coronavírus para intensificar suas atividades.

Levantamento feito pela FEBRABAN (Federação Brasileira de Bancos) mostra o crescimento de tentativas de várias modalidades de fraudes em janeiro e fevereiro de 2021 em comparação com o primeiro bimestre do ano passado.

1. Levantamento preliminar aponta que o volume de ocorrências do golpe da falsa central telefônica e do falso funcionário, por exemplo, aumentou cerca de 340%.

2. Também merecem destaque os ataques de *phishing*, cujo total de registros dobrou de um ano para o outro.

3. A incidência do golpe do falso motoboy, outra fraude muito comum durante a pandemia, se mantém como uma das principais investidas dos fraudadores no primeiro bimestre de 2021.

Os golpes mencionados acima são exemplos de fraudes que usam engenharia social, que consiste na manipulação psicológica do usuário para que ele forneça informações confidenciais, como senhas e números de cartões, para os criminosos, ou faça transações em favor das quadrilhas. Atualmente, 70% das fraudes estão vinculadas à engenharia social.

A FEBRABAN e seus bancos investem constantemente e de maneira massiva em campanhas e ações de conscientização em seus canais de comunicação com os clientes para orientar a população a se prevenir de fraudes.

Além da realização de campanhas educativas, os bancos investem cerca de R$ 2 bilhões por ano em sistemas de tecnologia da informação (TI) voltados para segurança – valor que corresponde a cerca de 10% dos gastos totais do setor com TI para garantir a tranquilidade de seus clientes em suas transações financeiras cotidianas.

“Para evitar ser vítima desse tipo de fraude, a orientação é ter cuidado ao compartilhar informações pessoais”, alerta Adriano Volpini, diretor da Comissão Executiva de Prevenção a Fraudes da FEBRABAN.

Abaixo, listamos alguns exemplos de golpes nos quais as pessoas são levadas a compartilhar seus dados com os golpistas que os utilizam para realizar operações fraudulentas.

Caso a pessoa seja vítima de um golpe como esses, a orientação é fazer um boletim de ocorrência e notificar o banco o quanto antes.

Conheça os principais golpes aplicados e como eles devem ser evitados

Golpe do Falso Funcionário do banco

O que é: O fraudador entra em contato com a vítima se passando por um falso funcionário do banco ou empresa com a qual o cliente tem um relacionamento ativo. O criminoso informa que há irregularidades na conta ou que os dados cadastrados estão incorretos. A partir daí, solicita os dados pessoais e financeiros da vítima. Com os dados em mãos, o fraudador realiza transações fraudulentas em nome do cliente.

Como evitar: O cliente deve sempre verificar a origem das ligações e mensagens recebidas contendo solicitações de dados. É importante ressaltar que o banco nunca liga para o cliente pedindo senha nem o número do cartão e também nunca liga para pedir para realizar uma transferência ou qualquer tipo de pagamento. Ao receber uma ligação suspeita, o cliente deve desligar, pegar o número de telefone que está no cartão e ligar de outro telefone para tirar a limpo essa história.

Phishing (pescaria digital)

O que é: O phishing, ou pescaria digital, é uma fraude eletrônica cometida pelos engenheiros sociais que visa obter dados pessoais do usuário. A forma mais comum de um ataque de phishing são as mensagens e e-mails falsos que induzem o usuário a clicar em links suspeitos. Também existem páginas falsas na internet que induzem a pessoa a revelar dados pessoais. Os casos mais comuns de phishing são e-mails recebidos de supostos bancos com mensagens que afirmam que a conta do cliente está irregular, ou o cartão ultrapassou o limite, ou que necessita revalidar seus pontos nos programas de fidelidade, atualizar token ou, ainda, que existe um novo software de segurança do banco que precisa ser instalado imediatamente pelo usuário.

Como evitar: Sempre verifique se o endereço da página de internet é o correto. Para garantir, não clique em links: digite o endereço no navegador. Além disso, nunca acesse links ou anexos de e-mails suspeitos. Mantenha seu sistema operacional e antivírus sempre atualizados. Sempre prefira comprar em sites conhecidos, e nunca use computadores públicos para comprar algo no comércio virtual. Não repasse a outra pessoa nenhum código

fornecido por SMS ou imagem de um QR Code enviado para autenticar alguma operação. Na dúvida, fale com seu banco.

Golpe do falso motoboy

O que é: O golpe começa com uma ligação ao cliente, de uma pessoa que se passa por funcionário do banco, e diz que o cartão foi clonado, informando que é preciso bloqueá-lo. Para isso, diz o golpista, bastaria cortá-lo ao meio e pedir um novo pelo atendimento eletrônico. O falso funcionário pede que a senha seja digitada no telefone, e fala que, por segurança, um motoboy irá buscar o cartão para uma perícia. O que o cliente não sabe é que, com o cartão cortado ao meio, o chip permanece intacto, e é possível realizar diversas transações.

Como evitar: Fique atento! Nenhum banco pede o cartão de volta ou envia qualquer pessoa ou portador para retirar o cartão na casa dos clientes. Então, desligue o telefone e ligue, de outro aparelho, para o banco, para verificar se realmente houve alguma irregularidade.

Golpe do falso leilão

O que é: O fraudador envia um link à vítima que simula um falso leilão. Para que possa ser dado um lance, a vítima tem que preencher formulários com seus dados pessoais e financeiros ou depositar um valor na conta do fraudador. Com dados como senha, número do cartão e CPF, o fraudador consegue fazer transações fraudulentas em nome do cliente.

Como evitar: O cliente nunca deve enviar dados, senhas e acessos a ninguém. É necessário sempre verificar a origem dos links recebidos antes de clicá-los. Além disso, deve-se verificar a veracidade do site de leilão e avaliações de outros usuários.

Golpe do WhatsApp

O que é: Os golpistas descobrem o número do celular e o nome da vítima de quem pretendem clonar a conta de WhatsApp. Com essas informações em mãos, os criminosos tentam cadastrar o WhatsApp da vítima nos aparelhos deles. Para concluir a operação, é preciso inserir o código de segurança que o aplicativo envia por SMS sempre que é instalado em um novo dispositivo. Os fraudadores enviam uma mensagem pelo WhatsApp fingindo ser do Serviço de Atendimento ao Cliente do site de vendas ou da empresa em que a vítima tem cadastro. Eles solicitam o código de segurança, que já foi enviado por SMS pelo aplicativo, afirmando se tratar de uma atualização, manutenção ou confirmação de cadastro. Com o código, os bandidos conseguem replicar a conta de WhatsApp em outro celular. A partir daí, os criminosos enviam mensagens para os contatos da pessoa, fazendo-se passar por ela, pedindo dinheiro emprestado.

Como evitar: Uma medida simples para evitar que o WhatsApp seja clonado é habilitar, no aplicativo, a opção "Verificação em duas etapas" Configurações/Ajustes > Conta > Verificação em duas etapas). Desta forma, é possível cadastrar uma senha que será solicitada periodicamente pelo app. Essa senha não deve ser enviada para outras pessoas ou digitadas em links recebidos.

Golpe do extravio do cartão

Como é: No trâmite de entrega do cartão até a vítima, fraudadores furtam a correspondência contendo este cartão. Depois, ligam para a vítima se passando por um funcionário do respectivo banco informando que houve problemas na entrega do cartão. Para a resolução deste suposto problema, solicitam à vítima a senha deste cartão. Com os dados descobertos, fazem transações em nome da vítima.

Como evitar: O cliente nunca deve enviar dados, senhas e acessos a ninguém. Também nunca deve preencher formulários na internet com dados pessoais e financeiros sem verificar a origem. Caso o prazo de entrega do cartão se esgote, é preciso informar o gerente sobre o atraso.

Golpe do delivery

Como é: O cliente faz seu pedido via aplicativo. O entregador apresenta uma maquininha com o visor danificado ou de uma forma que impossibilite a visualização do preço cobrado na tela, sendo um valor acima do real cobrado. Só depois de algum tempo, a vítima percebe que efetuou um pagamento elevado.

Como evitar: O cliente deve sempre checar o preço cobrado no visor da maquininha e nunca deve aceitar maquininhas onde os valores que são cobrados não estejam visíveis. De preferência em fazer o pagamento via aplicativo e não no momento da entrega.

Adriana Mompean
Diretoria de Comunicação
55 11 3244-9929 | 3186-9929
FEBRABAN | Federação Brasileira de Bancos
www.febraban.org.br

De: Nathalia Afonso <nathalia@lupa.news>
Enviada em: segunda-feira, 12 de julho de 2021 20:17
Para: Imprensa FEBRABAN <imprensa.febraban@febraban.org.br>
Assunto: Levantamento que fala sobre golpes - Agência Lupa

Caros, boa tarde.

Vi que a Febraban tem um levantamento que indica que, entre janeiro e fevereiro de 2021, foi registrado aumento de 100% nos ataques de phishing, a chamada pescaria digital, em relação ao mesmo período de 2020. Nessa modalidade, o usuário fornece informações pessoais em mensagens e e-mails falsos.

Seria possível me encaminhar esse levantamento? Eu não consegui encontrar ele na íntegra.

Link: https://g1.globo.com/jornal-nacional/noticia/2021/04/16/golpes-e-fraudes-por-telefone-e-e-mail-disparam-no-brasil-durante-a-pandemia.ghtml

Obrigada pela atenção. Preciso de um retorno até amanhã às 14h.

Abraços,

Nathália Afonso

Repórter

Lupa

nathalia@lupa.news

https://ddec1-0-en-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.lupa.news&umid=0e119a8c-ea64-46d3-9576-a4501b8e00e5&auth=eb780f9ad21ddc5cc88a09416af141930f96a56e-

09ce74501f3756190dbacd7bbdb84f6cb02810ac

[Texto das mensagens anteriores oculto]